

1 CLAIMS

2 What is claimed is:

3 1. A method of implementing a cellular automata based random number  
4 generator (CA-based RNG), comprising:

5 determining an interconnection topology;

6 screening a CA-based RNG candidate based on said interconnection topology;

7 and

8 subjecting said CA-based RNG candidate to a suite of random number tests in  
9 response to said CA-based RNG passing said screening step.

10

11 2. The method of claim 1, wherein said CA-based RNG candidate is  
12 under a periodic boundary condition in at least one dimension.

13

14 3. The method of claim 1, wherein said interconnection topology is  
15 identical for all cells of said CA-based RNG candidate.

16

17 4. The method of claim 1, wherein said determining topology (310) step  
18 includes:

19 exhaustively providing all possible interconnection topologies for a given  
20 neighborhood number for cells of said CA-based RNG candidate.

21

1           5.     The method of claim 4, wherein said determining topology (310) step  
2 further includes:

3           pruning said interconnection topologies to reject interconnection topologies  
4 for which no input of a cell of said CA-based RNG candidate is connected to said  
5 cell's output.

6  
7           6.     The method of claim 4, wherein said determining topology (310) step  
8 further includes:

9           pruning said interconnection topologies to reject interconnection topologies  
10 for which displacement values for all inputs for a cell are evenly divisible by a length  
11 of said CA-based RNG for any displacement values whose absolute value is greater  
12 than 1.

13  
14           7.     The method of claim 1, wherein said screening (320) step includes:  
15           calculating entropy of said CA-based RNG candidate; and  
16           accepting said CA-based RNG candidate for testing based on one or more  
17 predetermined criteria.

18  
19           8.     The method of claim 7, wherein said calculating entropy step includes:  
20           calculating an expected value of a subsequence within a sequence;  
21           initializing said CA-based RNG candidate through a predetermined number of  
22 clock cycles and monitoring occurrences of said subsequence; and  
23           determining said entropy based on said expected value and results of  
24 monitoring said subsequence occurrences.

25

1           9.     The method of claim 8, further comprising:  
2           rejecting said CA-based RNG in response said occurrence being greater than a  
3           multiple of said expected value.  
4

5           10.    The method of claim 7, wherein said accepting step includes accepting  
6           said CA-based RNG candidate for testing in response to said CA-based RNG  
7           candidate being in a list of a predetermined number of highest entropy CA-based  
8           RNG candidates.  
9

10          11.    The method of claim 10, wherein said accepting step includes  
11          accepting said CA-based RNG candidate for testing in response to said entropy of  
12          said CA-based RNG candidate being at or above a predetermined threshold entropy.  
13

14          12.    The method of claim 1, wherein said standardized suite of random  
15          number tests includes the DIEHARD suite of tests.  
16

17          13.    The method of claim 1, further comprising:  
18          selecting said CA-based RNG candidate in response to said CA-based RNG  
19          candidate passing said suite of random number tests without at least one of time  
20          spacing and site spacing.  
21

22          14.    A cellular automata based random number generator (CA-based RNG)  
23          implementing-module, comprising:

24                an     interconnection-topology-determining-module     determining     an  
25          interconnection topology;

1           a screening-module screening a CA-based RNG candidate based on said  
2 interconnection topology; and  
3           a testing-module subjecting said CA-based RNG candidate through a suite of  
4 tests in response to said CA-based RNG passing through said screening-module.  
5

6           15.    The CA-based RNG implementing-module of claim 13, wherein said  
7 screening-module comprises:

8           an entropy-calculating-module calculating entropy of said CA-based RNG  
9 candidate; and

10          a sorting-module accepting or rejecting said CA-based RNG candidate for  
11 testing based on a predetermined criteria.  
12

13          16.    The CA-based RNG implementing-module of claim 15, wherein said  
14 entropy-calculating-module comprises:

15          an expected-value-module calculating an expected count value of  
16 subsequences within a sequence;

17          an accumulating-module accumulating actual counts of said subsequences;  
18 and

19          an entropy-determining-module determining said entropy based on an output  
20 or outputs of said accumulating-module;  
21

22          17.    The CA-based RNG implementing-module of claim 15, wherein said  
23 sorting-module accepts said CA-based RNG candidate for testing in response to said  
24 CA-based RNG candidate being in a list of a predetermined number of highest  
25 entropy CA-based RNG candidates.

1

2           18.    The CA-based RNG implementing-module of claim 15, wherein said  
3    sorting-module accepts said CA-based RNG candidate for testing in response to said  
4    entropy of said CA-based RNG candidate being at or above a predetermined threshold  
5    entropy.

6

7           19.    The CA-based RNG implementing-module of claim 14, wherein said  
8    interconnection-topology-determining-module comprises:

9           a topology-generation-module generating one or more interconnection  
10   topologies; and

11          a topology-pruning-module pruning said interconnections based on one or  
12   more predetermined criteria.

13

14           20.    The CA-based RNG implementing-module of claim 19, wherein said  
15   topology-generation-module exhaustively provides all possible interconnection  
16   topologies for a given neighborhood number for cells of said CA-based RNG  
17   candidate.

18

19           21.    The CA-based RNG implementing-module of claim 19, topology-  
20   pruning-module prunes said interconnection topologies to reject interconnection  
21   topologies for which no input of a cell of said CA-based RNG candidate is connected  
22   to said cell's output.

23

24           22.    The CA-based RNG implementing-module of claim 19, topology-  
25   pruning-module prunes said interconnection topologies to reject interconnection

- 1 topologies for which displacement values for all inputs for a cell are evenly divisible
- 2 by a length of said CA-based RNG for any displacement values whose absolute value
- 3 is greater than 1.

HP  
Docket  
No.:  
10017475-1